

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Yuusaku OHTA et al. :  
Serial No. NEW : **Attn: Application Branch**  
Filed December 18, 2001 : **Attorney Docket No. 2001\_1828A**



SECURITY COMMUNICATION PACKET  
PROCESSING APPARATUS AND THE  
METHOD THEREOF

THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEE FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975.

**CLAIM OF PRIORITY UNDER 35 USC 119**

Assistant Commissioner for Patents,  
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2000-391938, filed December 25, 2000, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Yuusaku OHTA et al.

By Michael S. Huppert

Michael S. Huppert  
Registration No. 40,268  
Attorney for Applicants

MSH/kjf  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
December 18, 2001

CERTIFIED COPY OF  
PRIORITY DOCUMENT

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年12月25日

出 願 番 号

Application Number:

特願2000-391938

出 願 人

Applicant(s):

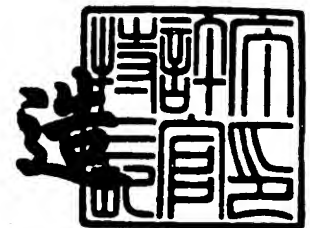
松下電器産業株式会社



2001年 9月13日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 2022520384

【提出日】 平成12年12月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00  
G09C 1/08

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 太田 雄策

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 山口 雅史

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 山内 弘貴

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

【代理人】

    【識別番号】 100097445

    【弁理士】

    【氏名又は名称】 岩橋 文雄

【選任した代理人】

    【識別番号】 100103355

    【弁理士】

    【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 セキュリティ通信パケット処理装置

【特許請求の範囲】

【請求項 1】 暗号処理用データブロックを処理するための暗号処理部と、認証処理用データブロックを処理するための認証処理部と、前記暗号処理用データブロックと暗号処理に必要な情報とを前記暗号処理部に出力し、前記認証処理用データブロックと認証処理に必要な情報とを前記認証処理部に出力し、前記暗号処理部と前記認証処理部とを制御する暗号認証処理制御部とを含むセキュリティ通信機能を有するネットワーク接続装置または前記セキュリティ通信機能を有するコンピュータにおいて、前記暗号処理部において処理されたデータブロックを認証処理用の最小データブロックサイズに等しくなるまで逐次的に蓄積し、前記認証処理用の最小データブロックサイズに等しくなるとこれを前記認証処理部に出力するデータブロック蓄積部を具備し、前記データブロック蓄積部の出力したデータブロックを前記認証処理部が処理している間に、前記暗号処理部は次の暗号処理用データブロックを処理し、前記データブロック蓄積部は次の認証処理用暗号処理済データブロックを蓄積することを特徴とするセキュリティ通信パケット処理装置。

【請求項 2】 暗号処理部と認証処理部の少なくともどちらか一方は 2 個以上であり、前記暗号処理部の数と等しいデータブロック蓄積部とを具備した、請求項 1 記載のセキュリティ通信パケット処理装置。

【請求項 3】 暗号認証処理制御部の処理命令により、前記暗号認証処理制御部より出力するデータブロックが暗号処理用データブロックであれば前記暗号認証処理制御部の出力部と暗号処理部の入力部を接続し、前記暗号認証処理制御部より出力するデータブロックが認証処理用データブロックであれば前記暗号認証処理制御部の出力部と認証処理部の入力部を接続し、前記暗号処理部で処理したデータブロックが更に認証処理も必要であれば前記暗号処理部の出力部とデータブロック蓄積部の入力部とを接続し、前記データブロック蓄積部で蓄積されたデータが出力できる状態になれば前記データブロック蓄積部の出力部と前記認証処理部の入力部とを接続するデータパス接続切替部を具備することを特徴とする請

求項 1 または 2 記載のセキュリティ通信パケット処理装置。

【請求項 4】 暗号処理部または認証処理部において処理されているデータブロックおよびデータブロック蓄積部に蓄積されているデータブロックを、暗号認証処理制御部の指示によりそのデータブロックに関する情報と共に一時的に退避させる処理データ退避部を、暗号処理部、認証処理部およびデータブロック蓄積部の一部、または全てに対して個別に設けた、請求項 1 から請求項 3 のいずれかに記載のセキュリティ通信パケット処理装置。

【請求項 5】 暗号処理部または認証処理部において処理されているデータブロックおよびデータブロック蓄積部に蓄積されているデータブロックを、暗号認証処理制御部の指示によりそのデータブロックに関する情報と共に一時的に退避させる処理データ退避部を、暗号処理部、認証処理部、データブロック蓄積部の任意の組み合わせで共通に設けた、請求項 1 から請求項 3 のいずれかに記載記載のセキュリティ通信パケット処理装置。

【請求項 6】 暗号処理用データブロックは 6 4 ビットであり、認証処理用データブロックは 5 1 2 ビットである、請求項 1 から請求項 5 のいずれかに記載のセキュリティ通信パケット処理装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、秘密通信時の高速化および低遅延化するためのセキュリティ通信パケット処理装置に関する。

【 0 0 0 2 】

【従来の技術】

近年、インターネットに代表される T C P / I P ネットワークが急速に普及しており、これに伴い電子音楽配信や W e b 上での商品の売買など、様々な形態のネットビジネスが脚光を浴び、次々に展開されつつある。このようなネットビジネスはサービス提供者側とユーザ側との間で信頼のおける安全な取引が行われることが大前提であるが、インターネットは常にクラッカーによる盗聴やなりすましなどからの危険にさらされており、一般に安全でないネットワークと考えられ

ている。そこで重要になってくるのが、電子認証や通信データの暗号化、ファイアウォールなどに代表されるネットワークセキュリティ技術である。これらは主にソフトウェアによる処理としてなされてきたが、将来的なTCP/IPインフラストラクチャの広帯域化に備え、暗号処理チップや暗号ボードなどのハードウェアによる高速処理の需要が高まりつつある。

#### 【0003】

ところで、IPSecに代表されるようなセキュリティ通信機能を有するコンピュータまたはネットワーク接続機器において、暗号処理と認証処理の両方を必要とするパケットに対しその処理を行う場合、図10で示される暗号、認証処理のフローチャートのように、まず平文パケットを暗号処理用データブロックに分割し、これを暗号処理した後、暗号化パケットとして再構築し、次にこの暗号化パケットを認証処理用データブロックとして分割し、これを認証処理した後、認証処理済パケットとして再構築を行っていた。

#### 【0004】

##### 【発明が解決しようとする課題】

しかし、上述の方法では、暗号処理と認証処理の両方を必要とするパケットに対しその処理を施す場合、暗号化パケットとして再構築する処理が冗長であった。このような冗長な処理は、暗号および認証の両処理を行う場合の処理の低速化、スループットの低減、暗号処理部または認証処理部の非効率的な使用につながるといった問題点があった。またこの方法では、あるパケットを暗号処理中に別の優先処理すべき平文パケットがある場合についてもこれを優先処理できないという問題点がある。また暗号処理部と認証処理部を各1つずつしか実装していない場合は複数のパケットの同時処理による高速スループットの実現は不可能であった。

#### 【0005】

本発明は、上記事情を考慮してなされたもので、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図ることができるセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 0 6 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、かつ複数のパケットの同時処理が可能なセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 0 7 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、かつ暗号処理部と認証処理部の各処理部の独立性を高めることにより、各処理部を柔軟に拡張、入れ替えを図ることが可能なセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 0 8 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、また複数のパケットの同時処理が可能で、かつ暗号処理部と認証処理部の各処理部の独立性を高めることにより、各処理部を柔軟に拡張、入れ替えを図ることが可能なセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 0 9 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、かつパケットの優先処理制御が可能なセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 1 0 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、また複数のパケットの同時処理が可能で、かつパケットの優先処理制御が可能なセキュリティ通信パケット処理装置を提供することを目的とする。

## 【 0 0 1 1 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延



化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、かつ暗号処理部と認証処理部の各処理部の独立性を高めることにより、各処理部を柔軟に拡張、入れ替えを図ることができ、かつパケットの優先処理制御が可能なセキュリティ通信パケット処理装置を提供することを目的とする。

#### 【 0 0 1 2 】

また、本発明は、暗号処理および認証処理の両方を行う場合の高速化、低遅延化、スループットの向上および暗号処理部と認証処理部の効率的な使用を図り、また複数のパケットの同時処理が可能で、かつ暗号処理部と認証処理部の各処理部の独立性を高めることにより、各処理部を柔軟に拡張、入れ替えを図ることが可能で、かつパケットの優先処理制御が可能なセキュリティ通信パケット処理装置を提供することを目的とする。

#### 【 0 0 1 3 】

##### 【課題を解決するための手段】

本発明の請求項 1 記載の発明は、暗号処理用データブロックを処理するための暗号処理部と、認証処理用データブロックを処理するための認証処理部と、前記暗号処理用データブロックと暗号処理に必要な情報とを前記暗号処理部に出力し、前記認証処理用データブロックと認証処理に必要な情報とを前記認証処理部に出力し、前記暗号処理部と前記認証処理部とを制御するための暗号認証処理制御部とを含むセキュリティ通信機能を有するネットワーク接続装置または前記セキュリティ通信機能を有するコンピュータにおいて、前記暗号処理部において処理されたデータブロックを認証処理用の最小データブロックサイズに等しくなるまで逐次的に蓄積し、前記認証処理用の最小データブロックサイズに等しくなるとこれを前記認証処理部に出力するデータブロック蓄積部を具備し、前記データブロック蓄積部の出力したデータブロックを前記認証処理部が処理している間に、前記暗号処理部は次の暗号処理用データブロックを処理し、前記データブロック蓄積部は次の認証処理用暗号処理済データブロックを蓄積することを特徴とするセキュリティ通信パケット処理装置であり、暗号処理と認証処理が必要なパケットに対してもその処理単位を暗号処理または認証処理に必要な十分なデータブロックを処理単位とすることにより、低遅延、スループットの向上を図ることができ

、かつ暗号処理部と認証処理部の効率的な使用を可能にするという作用を有する。

## 【 0 0 1 4 】

本発明の請求項 2 記載の発明は、暗号処理部と認証処理部の少なくともどちらか一方は 2 個以上設け、前記暗号処理部の数と等しいデータブロック蓄積部とを設けることにより、複数のパケットの並列処理を可能にし、スループットの高いセキュリティ処理を行えるという作用を有する。

## 【 0 0 1 5 】

本発明の請求項 3 記載の発明は、請求項 1 または 2 記載のセキュリティ通信パケット処理装置において、暗号認証処理制御部の処理命令により、前記暗号認証処理制御部より出力するデータブロックが暗号処理用データブロックであれば前記暗号認証処理制御部の出力部と暗号処理部の入力部を接続し、前記暗号認証処理制御部より出力するデータブロックが認証処理用データブロックであれば前記暗号認証処理制御部の出力部と認証処理部の入力部を接続し、前記暗号処理部で処理したデータブロックが更に認証処理も必要であれば前記暗号処理部の出力部とデータブロック蓄積部の入力部とを接続し、前記データブロック蓄積部で蓄積されたデータが出力できる状態になれば前記データブロック蓄積部の出力部と前記認証処理部の入力部とを接続するデータパス接続切替部を設けることにより、暗号処理部または認証処理部またはその両方が複数個ある場合でも、必ずしも暗号処理部とデータブロック蓄積部と認証処理部はそれぞれ 1 対 1 に対応する必要はなく、暗号処理後に認証処理の必要なデータブロックは、任意のデータブロック蓄積部へと出力することができ、データブロック蓄積部の出力は任意の認証処理部へと出力できるため、暗号処理部とデータブロック蓄積部と認証処理部のより効率的な使用が可能となり、また暗号処理部と認証処理部の拡張、入替が容易になるという作用を有する。

## 【 0 0 1 6 】

本発明の請求項 4 記載の発明は、請求項 1 から請求項 3 のいずれかに記載のセキュリティ通信パケット処理装置において、暗号処理部または認証処理部において処理されているデータブロックおよびデータブロック蓄積部に蓄積されている

データブロックを、暗号認証処理制御部の指示によりそのデータブロックに関する情報と共に一時的に退避させる処理データ退避部を、暗号処理部、認証処理部およびデータブロック蓄積部の一部、または全てに対して個別に設けることにより、パケットの優先処理を可能にするという作用を有する。

## 【 0 0 1 7 】

本発明の請求項 5 記載の発明は、請求項 1 から請求項 3 のいずれかに記載のセキュリティ通信パケット処理装置において、暗号処理部または認証処理部において処理されているデータブロックおよびデータブロック蓄積部に蓄積されているデータブロックを、暗号認証処理制御部の指示によりそのデータブロックに関する情報と共に一時的に退避させる処理データ退避部を、暗号処理部、認証処理部、データブロック蓄積部の任意の組み合わせで共通に設けたもので、処理データ退避部に接続された任意の暗号処理部、認証処理部またはデータブロック蓄積部は一つの処理データ退避部を利用することができ、また処理データ退避部にある処理途中のデータブロックは処理データ退避部に接続された任意の暗号処理部、認証処理部またはデータブロック蓄積部によって処理を再開できること可能にするという作用を有する。

## 【 0 0 1 8 】

本発明の請求項 6 記載の発明は、請求項 1 から請求項 5 のいずれかに記載のセキュリティ通信パケット処理装置において、暗号処理用データブロックは 6 4 ビットであり、認証処理用データブロックは 5 1 2 ビットであり、データブロック蓄積部は暗号処理済のデータブロックを 8 個蓄積するとこれを認証処理部に出力するという作用を有する。

## 【 0 0 1 9 】

## 【発明の実施の形態】

以下、本発明の実施の形態を、図 1 ～図 6 を参照して、詳細に説明する。

## 【 0 0 2 0 】

## (実施の形態 1)

図 1 に、本発明の実施の形態 1 におけるセキュリティ通信パケット処理装置のブロック図を示す。本実施の形態では、暗号認証処理制御部 0 1 0 1、暗号処理

部 0 1 0 2、データブロック蓄積部 0 1 0 3 および認証処理部 0 1 0 4 が図 1 のように接続されている場合について説明する。

#### 【 0 0 2 1 】

本実施の形態において暗号認証処理制御部 0 1 0 1 に入力されるパケットは、そのパケットに対して施すべき処理内容から 4 つに分類される。すなわち 1 種類目として暗号処理と認証処理の必要な送信用パケット、2 種類目として復号処理と認証処理の必要な受信パケット、3 種類目として暗号処理あるいは復号処理のみが必要なパケット、そして最後に 4 種類目として認証処理のみが必要なパケットである。以下ではこの 4 種類のパケットのそれぞれの処理の詳細について説明する。

#### 【 0 0 2 2 】

まず最初に暗号処理と認証処理の必要な送信パケットの処理過程について説明する。この場合、まず第 1 のステップとして、暗号認証処理制御部 0 1 0 1 は処理すべきパケットとそのパケットに施すべき処理に必要な情報を受け取る。ここでパケットに施すべき処理に必要な情報とは、暗号処理の是非、認証処理の是非、暗号処理を行うのであれば、そのアルゴリズム、鍵情報、I V、暗号化処理を行うのか復号化処理を行うのかという情報、認証処理を行うのであればそのアルゴリズムや必要に応じてその鍵情報、認証値などを含む。またここで暗号アルゴリズムとしては D E S や 3 D E S を含む。また認証アルゴリズムとしては H M A C - M D 5 - 9 6 や H M A C - S H A - 1 - 9 6 を含む。

#### 【 0 0 2 3 】

また、パケットとそのパケットに施すべき処理情報は識別番号などで対応づけられており、複数のパケットが連続的に暗号認証処理制御部 0 1 0 1 に入力されてもそれらを混同しないような仕組みが保証されている。暗号認証処理制御部 0 1 0 1 はパケットの処理情報から、そのパケットを暗号処理と認証処理の必要な送信パケットであると判断すると、まず暗号処理用のデータブロックに分割し、そのパケットの処理情報を含めた形で暗号処理部 0 1 0 2 に送る。

#### 【 0 0 2 4 】

第 2 のステップとして、暗号処理部 0 1 0 2 は暗号処理に必要な情報と暗号処

理用データブロックを暗号認証処理制御部 0 1 0 1 から受け取ると、暗号処理情報からそのブロックに対して適用すべき暗号アルゴリズム、鍵、I V、暗号化あるいは復号化の処理方法などを判断し、その処理方法にしたがって暗号処理用ブロックを処理する。ここで暗号処理部 0 1 0 2 では複数の暗号アルゴリズムの処理が可能ないように実現されていてもよい。処理された暗号処理済ブロックは本実施の形態の出力として出力されると同時に、認証処理が必要なので、認証処理に必要な情報と共にデータブロック蓄積部 0 1 0 3 にも出力される。

#### 【 0 0 2 5 】

第 3 のステップとして、データブロック蓄積部 0 1 0 3 では暗号処理部 0 1 0 2 より出力された暗号処理済のデータブロックを認証処理に必要なデータブロックサイズに等しくなるまで逐次的に蓄積し、認証処理に必要なデータブロックサイズに等しくなると、認証処理部 0 1 0 4 にその処理情報と共に出力する。データブロック蓄積部 0 1 0 3 は、蓄積された暗号処理済のデータブロックの蓄積量が認証用データブロックのサイズに等しいか否かの蓄積状況を、データブロック蓄積部 0 1 0 3 が持つ蓄積ブロックカウンタによりカウントすることで判断する。また、別の方法としては、蓄積ブロックカウンタを暗号認証処理制御部 0 1 0 1 が持つという方法も考えられる。

#### 【 0 0 2 6 】

第 4 のステップとして、認証処理部 0 1 0 4 はデータブロック蓄積部 0 1 0 3 から暗号処理済の認証処理用データブロックとその処理情報を受け取り、その処理情報に従って認証処理を行い、その認証値を計算する。認証処理部 0 1 0 4 は現在処理中のパケットの認証値をその出力とする。また、暗号処理部 0 1 0 2 は次の暗号処理用データブロックが入力されるとこの処理を行う。またデータブロック蓄積部 0 1 0 3 は次の認証処理用暗号処理済データブロックが入力されればこれを蓄積する。以上第 1 から第 4 のステップを暗号処理と認証処理の両方が必要な送信パケットに繰り返し適用することにより、このパケットは暗号処理と認証処理が施される。

#### 【 0 0 2 7 】

次に、先に述べた第 2 の種類のパケット、すなわち復号処理と認証処理の必要

な受信パケットの処理過程についてその詳細を説明する。この場合、まず第1のステップとして、暗号認証処理制御部0101は処理すべきパケットとその処理情報を受け取り、その処理情報から復号処理と認証処理の必要な受信パケットであることを判断すると、このパケットを複製し、一つは復号処理用のパケットとして復号処理用のデータブロックに分割し、暗号処理部0102にその処理情報と共に出力する。もう一つのパケットは、認証処理用のパケットとして認証処理用のデータブロックに分割し、認証処理部0104にその処理情報と共に出力する。

#### 【0028】

次に第2のステップとして、以下の2つの処理を平行して行う。すなわち1つ目として、暗号処理部0102は受け取った復号処理用のデータブロックを、その処理情報を元に復号し、本実施の形態の出力として出力する。2つ目として認証処理部0104は受け取った認証処理用のデータブロックを認証処理し、その認証値を計算する。以上、第1と第2のステップを復号処理と認証処理の両方が必要な受信パケットに繰り返し適用することにより、このパケットは復号処理と認証処理が施される。

#### 【0029】

次に、先に述べた第3の種類のパケット、すなわち暗号処理あるいは復号処理の必要なパケットの処理過程についてその詳細を説明する。この場合、まず第1のステップとして、暗号認証処理制御部0101は処理すべきパケットとその処理情報を受け取り、その処理情報から暗号処理または復号処理のみが必要なパケットであることを判断すると、これを暗号処理用データブロックに分割し、その処理情報と共に暗号処理部0102に出力する。

#### 【0030】

次に第2のステップとして暗号処理用データブロックとその処理情報を受け取った暗号処理部0102はその処理情報に従って暗号処理あるいは復号処理を行い、本実施の形態の出力として処理済データブロックを出力する。以上、第1と第2のステップを暗号処理または復号処理のみが必要なパケットに繰り返し適用することにより、このパケットは暗号処理または復号処理が施される。

## 【 0 0 3 1 】

次に、先に述べた第4の種類のパケット、すなわち認証処理のみが必要なパケットの処理過程についてその詳細を説明する。この場合、まず第1のステップとして、暗号認証処理制御部0101は処理すべきパケットとその処理情報を受け取り、その処理情報から認証処理のみが必要なパケットであることを判断すると、これを認証処理用データブロックに分割し、その処理情報と共に認証処理部0104に出力する。

## 【 0 0 3 2 】

次に第2のステップとして認証処理用データブロックとその処理情報を受け取った認証処理部0104はその処理情報に従って認証処理を行い、認証値を計算する。以上、第1と第2のステップを認証処理のみが必要なパケットに繰り返し適用することにより、このパケットは認証処理が施される。

## 【 0 0 3 3 】

本実施の形態において暗号認証処理制御部0101、暗号処理部0102、データブロック蓄積部0103および認証処理部0104の間のデータの受け渡し方法については例えば各処理部間での2WAYハンドシェイクによる方法がある。本実施の形態はLSIやFPGAにより実現されても良いし、暗号処理部0102や認証処理部0104をDSPにより実現する形態でもよい。

## 【 0 0 3 4 】

また本実施の形態においては、データブロック蓄積部0103は認証処理部0104と独立な構成として設けたが、必ずしもこの構成に限定されるものではなく、データブロック蓄積部0103は認証処理部0104に含まれる形で設けてもよい。

## 【 0 0 3 5 】

本実施の形態は、IETF (Internet Engineering Task Force)が発行するRequest For Comments 2401~2410で公開されているIPセキュリティの仕様にも対応できる。上記のように本発明の実施の形態1では、データブロック蓄積部0103を設けることにより、暗号処理部0102、認証処理部0104には常にその処理に必要十分なサイズのデータブロックが入力される仕組みになっている

## 【 0 0 3 6 】

従って、従来のように暗号処理と認証処理の両方が必要な送信パケットについて、まず暗号処理を行い、暗号処理済のパケットとして一度構築した後に再度認証処理用のデータブロックに分割し認証処理を行う方法では、暗号処理後と認証処理後の2回パケットを構築する必要がある、認証処理部0104は暗号処理済のデータブロックがパケットとして再構築されるまで待つ必要があったが、本実施の形態では、暗号処理部0102と認証処理部0104の間にデータブロック蓄積部0103を設けることにより、分割されたパケットの再構築はどのようなセキュリティ処理に対しても1回で済み、認証処理部0104は暗号処理済のデータブロックが認証処理に必要なデータブロックのサイズに等しくなるまで蓄積されるとこれを認証処理部に出力するため、認証処理部0104は従来の方法に比べ処理待ちの時間が短縮される。以上より、パケットのセキュリティ処理のスループットの向上、低遅延化、高速化および暗号処理部と認証処理部の効率的な使用が可能となる。

## 【 0 0 3 7 】

## (実施の形態2)

図2に、本発明の実施の形態2におけるセキュリティ通信パケット処理装置のブロック図を示す。本実施の形態は、暗号処理部または認証処理部の少なくともどちらか一方が2つ以上であり、暗号処理部と等しい数のデータブロック蓄積部を有することを特徴とする。具体的な構成例としては、1つの暗号処理部と1つのデータブロック蓄積部、および1つの認証処理部を組み合わせたものを2組並列に並べた構成が挙げられる。図2はこの場合の構成図である。

## 【 0 0 3 8 】

本実施の形態では各暗号処理部、各認証処理部および各データブロック蓄積部にはそれぞれを一意に識別するためのID番号が割り当てられている。また暗号認証処理制御部0201は各処理部が処理中であるか処理待ちであるかといった処理状況を、例えば処理中であることを意味するBUSY信号や処理待ちであることを意味するREADY信号を各処理部から受け取ることにより把握している



。ここで例えば2つの暗号処理部が同時に処理待ち状態にある場合、暗号処理に必要なデータはID番号の小さい方で処理を行う。2つの認証処理部が同時に処理待ち状態にある場合についても同様である。

#### 【0039】

但し、暗号処理と認証処理に必要な送信パケットについて、暗号処理を暗号処理部0202bで行った場合、暗号処理済のデータブロックはデータブロック蓄積部0203bに蓄積され認証処理部0204bに入力される。すなわち、暗号処理と認証処理に必要な送信パケットについてはデータブロック蓄積部、認証処理部はどの暗号処理部に処理されたかに依存する。

#### 【0040】

従って、暗号認証処理制御部0201は、暗号処理、認証処理、またはその両方の処理に必要なパケットとそのパケットに対する処理情報を受け取ると、そのパケットが暗号処理が必要であれば処理待ち状態にある暗号処理部にその処理情報と共に出力し、認証処理のみが必要であれば処理待ち状態にある認証処理部にその処理情報と共に出力する。以降の処理は実施の形態1で述べた方法に従う。

#### 【0041】

本実施の形態では1組の暗号処理部、認証処理部、データブロック蓄積部を2つ並列に並べた構成について説明したが、必ずしも上記の構成に限定されるものではなく、例えば暗号処理部の処理性能の和と認証処理部の処理性能の和が等しくなるように暗号処理部と認証処理部を配置するような構成が挙げられる。この場合、暗号処理部と認証処理部の数の比は、暗号処理用データブロックのサイズをB、認証処理用データブロックのサイズをmB、暗号処理部の1ブロックあたりの処理ステップ数をT1、認証処理部の1ブロックあたりの処理ステップ数をT2とすると、暗号処理部数：認証処理部数＝T2：mT1として求められる。ここでB、m、T1、T2は全て自然数である。

#### 【0042】

上記のように本発明の実施の形態2では、暗号処理部または認証処理部の少なくともどちらか一方を2つ以上具備することにより、パケットの並列処理を実現できる。

## 【 0 0 4 3 】

## (実施の形態 3)

図 3 に、本発明の実施の形態 3 におけるセキュリティ通信パケット処理装置のブロック図を示す。本実施の形態は、暗号認証処理制御部 0 3 0 1、データパス接続切替部 0 3 0 2、暗号処理部 0 3 0 3 a、0 3 0 3 b、データブロック蓄積部 0 3 0 4 a、0 3 0 4 b および認証処理部 0 3 0 5 a、0 3 0 5 b が図 3 のように接続された構成となっている。

## 【 0 0 4 4 】

本実施の形態において、暗号認証処理制御部 0 3 0 1 に入力されるパケットの種類としては、実施の形態 1 で述べた 4 種類のパケットが挙げられる。以下において、この 4 種類のパケットの具体的な処理過程を述べる。

## 【 0 0 4 5 】

まず、第 1 の種類のパケットとして、暗号処理と認証処理の必要な送信パケットの処理過程について説明する。この場合、第 1 のステップとしてまず暗号認証処理制御部 0 3 0 1 は処理すべきパケットとその処理情報を受け取り、処理情報の内容から、暗号処理と認証処理の必要な送信パケットであることを判断すると、どの暗号処理部、データブロック蓄積部、認証処理部が処理待ち状態にあるかを実施の形態 2 で述べた方法により判断する。

## 【 0 0 4 6 】

ここで例えば暗号処理部 0 3 0 3 b、データブロック蓄積部 0 3 0 4 b および認証処理部 0 3 0 5 b が処理待ち状態にあったとすると、第 2 のステップとして暗号認証処理制御部 0 3 0 1 は、データパス接続切替部 0 3 0 2 に対し、暗号認証処理部 0 3 0 1 の出力部と暗号処理部 0 3 0 3 b の入力部を接続する命令、暗号処理部 0 3 0 3 b の出力部とデータブロック蓄積部 0 3 0 4 b の入力部を接続する命令およびデータブロック蓄積部 0 3 0 3 b の出力部と認証処理部 0 3 0 5 b の入力部を接続する命令を出す。ここで接続命令とは接続すべき各処理部の I D 番号により表されたものや、セレクタの制御信号のようなものであっても良い。データパス接続切替部 0 3 0 2 は接続が完了すると暗号認証処理制御部 0 3 0 1 に接続完了の意味を表す R E A D Y 信号を出力する。

## 【 0 0 4 7 】

第 3 のステップとして、暗号認証処理制御部 0 3 0 1 はデータパス接続切替部 0 3 0 2 から R E A D Y 信号を受け取ると処理すべきパケットを暗号処理用のデータブロックに分割し、これを接続された暗号処理部 0 3 0 3 b にその処理情報と共に出力する。以降の処理は実施の形態 1 で述べた方法にしたがって行われる。

## 【 0 0 4 8 】

次に第 2 の種類のパケット、つまり復号処理と認証処理の必要な受信パケットについて、その処理過程を説明する。この場合、第 1 のステップとしてまず暗号認証処理制御部 0 3 0 1 は処理すべきパケットとその処理情報を受け取り、処理情報の内容から、復号処理と認証処理の必要な受信パケットであることを判断すると、どの暗号処理部、認証処理部が処理待ち状態にあるかを判断する。ここで例えば暗号処理部 0 3 0 3 b および認証処理部 0 3 0 5 b が処理待ち状態にあったとすると、第 2 のステップとして暗号認証処理制御部 0 3 0 1 は、データパス接続切替部 0 3 0 2 に対し、暗号認証処理制御部 0 3 0 1 の出力部と暗号処理部 0 3 0 3 b の入力部を接続する命令、暗号認証処理制御部 0 3 0 1 の出力部と認証処理部 0 3 0 5 b の入力部を接続する命令を出す。

## 【 0 0 4 9 】

第 3 のステップとして、命令を受けたデータパス接続切替部 0 3 0 2 は命令情報を元に暗号認証処理制御部 0 3 0 1 と暗号処理部 0 3 0 3 b を接続し、また暗号認証処理制御部 0 3 0 1 と認証処理部 0 3 0 5 b を接続し、接続完了後、暗号認証処理制御部 0 3 0 1 に対し、R E A D Y 信号を出力する。第 4 のステップとして、暗号認証処理制御部 0 3 0 1 は実施の形態 1 で述べた方法と同様にパケットを複製して、1 つは暗号処理用データブロックに分割し暗号処理部 0 3 0 3 b へ、もう 1 つは認証処理用データブロックに分割して認証処理部 0 3 0 5 b へ出力する。以降の処理は実施の形態 1 で述べた方法にしたがって行われる。

## 【 0 0 5 0 】

次に第 3 の種類のパケット、つまり暗号または復号処理の必要なパケットについてその処理過程を説明する。この場合、第 1 のステップとしてまず暗号認証処

理制御部 0 3 0 1 は処理すべきパケットとその処理情報を受け取り、処理情報の内容から、暗号処理または復号処理の必要なパケットであることを判断すると、どの暗号処理部が処理待ち状態にあるかを判断する。ここで例えば暗号処理部 0 3 0 3 b が処理待ち状態にあったとすると、第 2 のステップとして暗号認証処理制御部 0 3 0 1 は、データパス接続切替部 0 3 0 2 に対し、暗号認証処理制御部 0 3 0 1 の出力部と暗号処理部 0 3 0 3 b の入力部を接続する命令を出す。

## 【 0 0 5 1 】

第 3 のステップとして、命令を受けたデータパス接続切替部 0 3 0 2 は命令情報を元に暗号認証処理制御部 0 3 0 1 と暗号処理部 0 3 0 3 b を接続し接続完了後、暗号認証処理制御部 0 3 0 1 に対し、READY 信号を出力する。第 4 のステップとして、暗号認証処理制御部 0 3 0 1 はパケットを暗号処理用データブロックに分割してこれを暗号処理部 0 3 0 3 b に出力する。以降の処理は実施の形態 1 で述べた方法にしたが行われる。

## 【 0 0 5 2 】

最後に第 4 の種類のパケット、つまり認証処理の必要なパケットについてその処理過程を説明する。この場合、第 1 のステップとしてまず暗号認証処理制御部 0 3 0 1 は処理すべきパケットとその処理情報を受け取り、処理情報の内容から、認証処理の必要なパケットであることを判断すると、どの認証処理部が処理待ち状態にあるかを判断する。ここで例えば認証処理部 0 3 0 5 b が処理待ち状態にあったとすると、第 2 のステップとして暗号認証処理制御部 0 3 0 1 は、データパス接続切替部 0 3 0 2 に対し、暗号認証処理制御部 0 3 0 1 の出力部と認証処理部 0 3 0 5 b の入力部を接続する命令を出す。

## 【 0 0 5 3 】

第 3 のステップとして、命令を受けたデータパス接続切替部 0 3 0 2 は命令情報を元に暗号認証処理制御部 0 3 0 1 と認証処理部 0 3 0 5 b を接続し接続完了後、暗号認証処理制御部 0 3 0 1 に対し、READY 信号を出力する。第 4 のステップとして、暗号認証処理制御部 0 3 0 1 はパケットを暗号処理用データブロックに分割してこれを認証処理部 0 3 0 5 b に出力する。以降の処理は実施の形態 1 で述べた方法にしたが行われる。

## 【 0 0 5 4 】

上記のように本発明の実施の形態 3 では、データバス接続切替部 0 3 0 2 を設けることにより、必ずしも 1 つの暗号処理部と 1 つのデータブロック蓄積部および 1 つの認証処理部が 1 対 1 に対応する必要はなく、ある暗号処理部の出力は処理待ち状態にある任意のデータブロック蓄積部へと出力でき、またデータブロック蓄積部の出力は処理待ち状態にある任意の認証処理部へと入力することが可能な構成になっており、暗号処理部、データブロック蓄積部および認証処理部の効率的な使用が可能となっている。また、暗号処理部や、認証処理部を複数設けたり、ある暗号アルゴリズムを実装した暗号処理部を別の暗号アルゴリズムを実装した暗号処理部で置き換えるなどの操作も容易に実現できる。

## 【 0 0 5 5 】

## (実施の形態 4)

図 4 に、本発明の実施の形態 4 におけるセキュリティ通信 packets 処理装置のブロック図を示す。本実施の形態は、実施の形態 3 で述べた構成において、暗号処理部 0 4 0 3 a、0 4 0 3 b、データブロック蓄積部 0 4 0 4 a、0 4 0 4 b および認証処理部 0 4 0 5 a、0 4 0 5 b のそれぞれに処理データ退避部 0 4 0 6 a、0 4 0 6 b、0 4 0 6 c、0 4 0 6 d、0 4 0 6 e および 0 4 0 6 f を設けた構成となっている。

## 【 0 0 5 6 】

本実施の形態において、暗号認証処理制御部 0 4 0 1 は、実施の形態 1 で述べた 4 種類の packets と、その処理情報を受け取る。ここで処理情報にはその packets の処理の優先度に関する情報が含まれている。優先度に関する情報とは、例えば数字で表現される。この数字は例えば IP ヘッダに含まれる Type of Service (T o S) ビットの情報を元に割り当てられる。本実施の形態では、以下のステップにしたがって処理を行う。

## 【 0 0 5 7 】

まず、第 1 のステップとして暗号認証処理制御部 0 4 0 1 は処理すべき packets とその処理情報を受け取ると、その処理情報から packets の処理に必要な処理部が処理待ち状態にあればそこに出力する。この場合の処理過程については実施

の形態3に従う。パケットの処理に必要な処理部がすべて処理中である場合、暗号認証処理制御部0401はもっとも優先度の低いパケットを処理している処理部に対し、現在処理中のデータをその処理部に接続された処理データ退避部に退避させる命令を出す。

#### 【0058】

第2のステップとして退避命令を受けた処理部は現在処理中のデータとその処理情報を処理データ退避部に退避させる。退避処理完了後、暗号認証処理制御部0401にREADY信号を出力する。第3のステップとして暗号認証処理制御部0401は、READY信号を受け取るとその処理部にデータブロックとその処理情報を出力する。以降の処理は実施の形態2で述べた方法に従う。

#### 【0059】

本実施の形態では全ての暗号処理部、データブロック蓄積部および認証処理部にそれぞれ処理データ退避部を設けた構成となっているが、必ずしも上記の構成に限定されるものではなく、例えば全ての暗号処理部のみにそれぞれ処理データ退避部を設けるなど、任意の処理部にそれぞれ処理データ退避部を設けても良い。また、本実施の形態は実施の形態2で述べた構成にも適用できる。この場合の処理方法については上記と同様の方法によって可能である。

#### 【0060】

上記のように本発明の実施の形態4では、処理データ退避部0406a、0406b、0406c、0406d、0406e、0406fを設けることにより、実施の形態3で述べた効果に加え、パケットの優先処理制御が実現できる。

#### 【0061】

##### (実施の形態5)

図5に、本発明の実施の形態5におけるセキュリティ通信パケット処理装置のブロック図を示す。本実施の形態は、実施の形態2で述べた構成において、暗号処理部0502a、0502b、データブロック蓄積部0503a、0503bおよび認証処理部0504a、0504bに処理データ退避部0505を共通に設けた構成となっている。本実施の形態では、暗号認証処理制御部0501は実施の形態4で述べた種類のパケットを受け取る。

## 【 0 0 6 2 】

本実施の形態では、以下のステップに従って処理を行う。まず第 1 のステップとして、暗号認証処理制御部 0 5 0 1 は処理すべきパケットとその処理情報を受け取ると、その処理情報からパケットの処理に必要な処理部が処理待ち状態であればそこに出力する。この場合の処理過程については実施の形態 2 に従う。パケットの処理に必要な処理部がすべて処理中である場合、暗号認証処理制御部 0 5 0 1 はもっとも優先度の低いパケットを処理している処理部に対し、現在処理中のデータを処理データ退避部 0 5 0 5 に退避させる命令を退避先のアドレスを含めた形で出す。

## 【 0 0 6 3 】

第 2 のステップとして退避命令を受けた処理部は現在処理中のデータとその処理情報を処理データ退避部 0 5 0 5 の指定されたアドレスに退避させる。退避処理完了後、暗号認証処理制御部 0 5 0 1 に R E A D Y 信号を出力する。以降の処理は実施の形態 4 で述べた方法に従う。

## 【 0 0 6 4 】

本実施の形態では全ての暗号処理部、データブロック蓄積部および認証処理部に共通に処理データ退避部を設けた構成となっているが、必ずしも上記の構成に限定されるものではなく、例えば全ての暗号処理部のみに共通に処理データ退避部を設けるなど、任意の組み合わせの処理部で処理データ退避部を共通に設けても良い。また、本実施の形態は実施の形態 3 で述べた構成にも適用できる。この場合の処理方法については上記と同様の方法によって可能である。

## 【 0 0 6 5 】

また、本実施の形態を実施の形態 3 に適用する場合、図 6 のように処理データ退避部 0 6 0 6 をデータパス接続切替部 0 6 0 2 に接続する形で具備しても良い。この場合、暗号認証処理制御部 0 6 0 1 はデータパス接続切替部 0 6 0 2 に処理中のデータを退避させるべき処理部と処理データ退避部 0 6 0 6 を接続する命令を出すことにより、データの退避が可能となる。

## 【 0 0 6 6 】

上記のように本発明の実施の形態 5 では、処理データ退避部 0 5 0 5 を暗号処

理部 0 5 0 2 a、0 5 0 2 b データブロック蓄積部 0 5 0 3 a、0 5 0 3 b 認証処理部 0 5 0 4 a、0 5 0 4 b に共通で設けることにより、実施の形態 4 で述べた効果に加え、処理データ退避部 0 5 0 5 の効率的な使用が可能となる。

## 【 0 0 6 7 】

## 【発明の効果】

以上で説明したように、本発明によれば、暗号処理と認証処理の両方の処理を行う場合の処理単位を、その処理を行うのに必要十分なデータブロックサイズとすることにより、同処理単位をパケットとしていた従来技術と比べ、暗号および認証処理の高速化および低遅延化が実現できる。

## 【 0 0 6 8 】

また、本発明によれば、暗号処理と認証処理の両方の処理を行う場合、暗号処理後のデータブロックは認証処理に必要なデータブロックサイズになるまで蓄積され、認証処理用のデータブロックに等しくなるとこれを認証処理するため、暗号処理後に一度パケットとして組み直していた従来技術と比べ、暗号処理後のデータブロックをバッファリングするためのメモリ資源の節約にも寄与できる。

## 【 0 0 6 9 】

また、本発明によれば、暗号処理部および認証処理部の少なくともどちらか一方を 2 つ以上設けることにより、複数のパケットの同時処理を可能にし、パケットのセキュリティ処理のスループット向上を実現できる。

## 【 0 0 7 0 】

また、本発明によれば、データパス接続切替部を設けることにより、暗号処理部または認証処理部またはその両方が複数個ある場合でも、必ずしも暗号処理部とデータブロック蓄積部と認証処理部はそれぞれ 1 対 1 に対応する必要はなく、暗号処理後に認証処理の必要なデータブロックは、任意のデータブロック蓄積部へと出力することができ、データブロック蓄積部の出力は任意の認証処理部へと出力できるため、暗号処理部とデータブロック蓄積部と認証処理部のより効率的な使用が可能となり、また暗号処理部と認証処理部の拡張、入替が容易になるという効果がある。



【 0 0 7 1 】

また、本発明によれば、処理データ退避部を設けることにより、パケット処理は必ずしもセキュリティ通信パケット処理装置に入力された順に処理されるわけではなく、パケットの優先度などに応じ、その処理順序を操作することができる。

【 0 0 7 2 】

また、本発明によれば、処理データ退避部を暗号処理部、認証処理部およびデータブロック蓄積部の任意の組み合わせで共有することにより、処理待ち状態にある、処理データ退避部を共有する任意の暗号処理部あるいは認証処理部は、処理データ退避部に処理すべきデータブロックがあればこれを処理することが可能なため、暗号処理部および認証処理部のより効率的な利用が可能となる。

【図面の簡単な説明】

【図 1】

実施の形態 1 でのセキュリティ通信パケット処理装置のブロック図

【図 2】

実施の形態 2 でのセキュリティ通信パケット処理装置の基本構成図

【図 3】

実施の形態 3 でのセキュリティ通信パケット処理装置の基本構成図

【図 4】

実施の形態 4 でのセキュリティ通信パケット処理装置の基本構成図

【図 5】

実施の形態 5 でのセキュリティ通信パケット処理装置の基本構成図

【図 6】

実施の形態 5 でのセキュリティ通信パケット処理装置の基本構成図

【図 7】

従来平文パケットに対する暗号処理および認証処理のフローチャート

【符号の説明】

0 1 0 1, 0 2 0 1, 0 3 0 1, 0 4 0 1, 0 5 0 1, 0 6 0 1 暗号認証処理制御部

0 3 0 2, 0 4 0 2, 0 6 0 2 データパス接続切替部

0 1 0 2, 0 2 0 2, 0 3 0 3, 0 4 0 3, 0 5 0 2, 0 6 0 3 暗号処理部

0 1 0 3, 0 2 0 3, 0 3 0 4, 0 4 0 4, 0 5 0 3, 0 6 0 4 データブロッ  
ク蓄積部

0 1 0 4, 0 2 0 4, 0 3 0 5, 0 4 0 5, 0 5 0 4, 0 6 0 5 認証処理部

0 4 0 6, 0 5 0 5, 0 6 0 6 処理データ退避部

7 0 1 セキュリティ処理開始

7 0 2 暗号処理の是非による分岐

7 0 3 暗号用データブロック分割

7 0 4 暗号処理

7 0 5 暗号化パケット構築

7 0 6 認証処理の是非による分岐

7 0 7 認証用データブロック分割

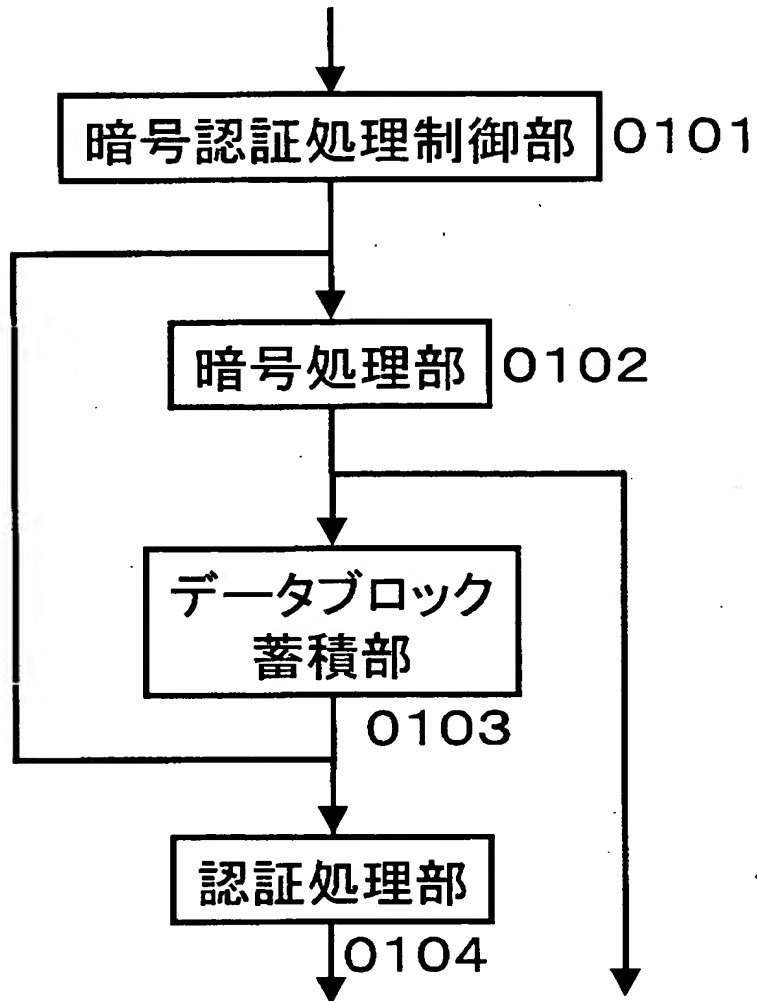
7 0 8 認証処理

7 0 9 認証処理済パケット構築

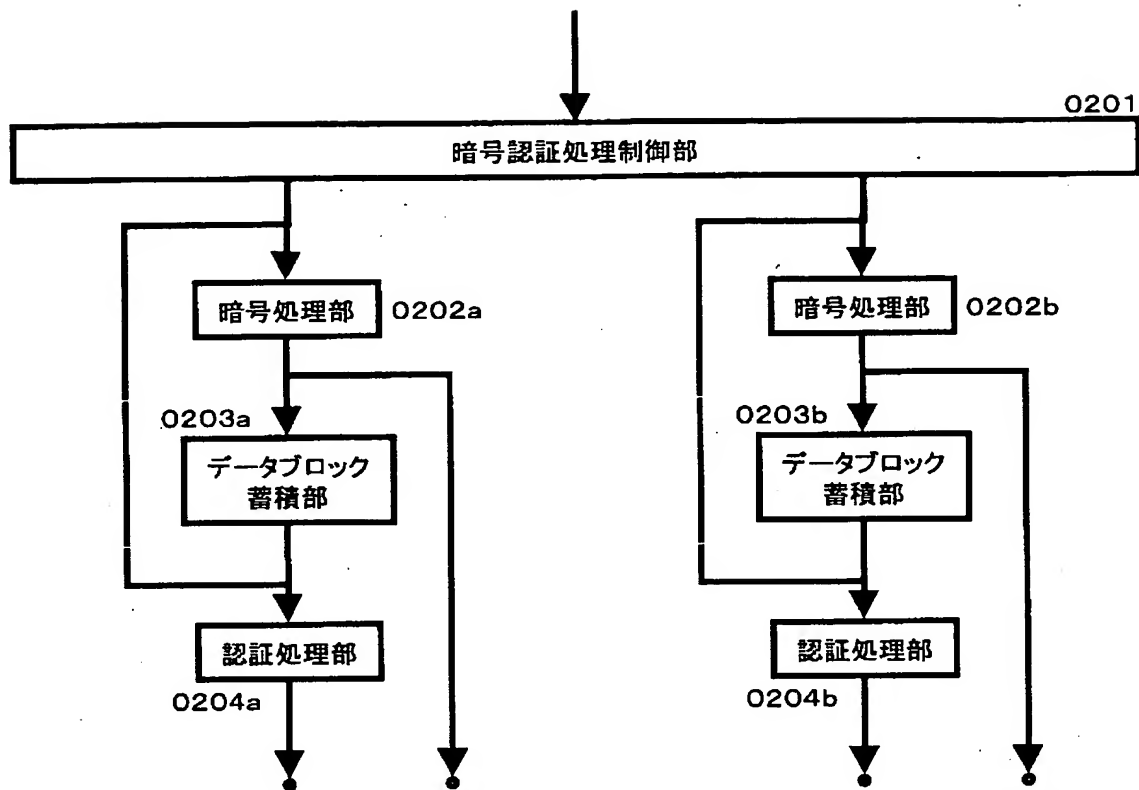
7 1 0 セキュリティ処理終了

【書類名】 図面

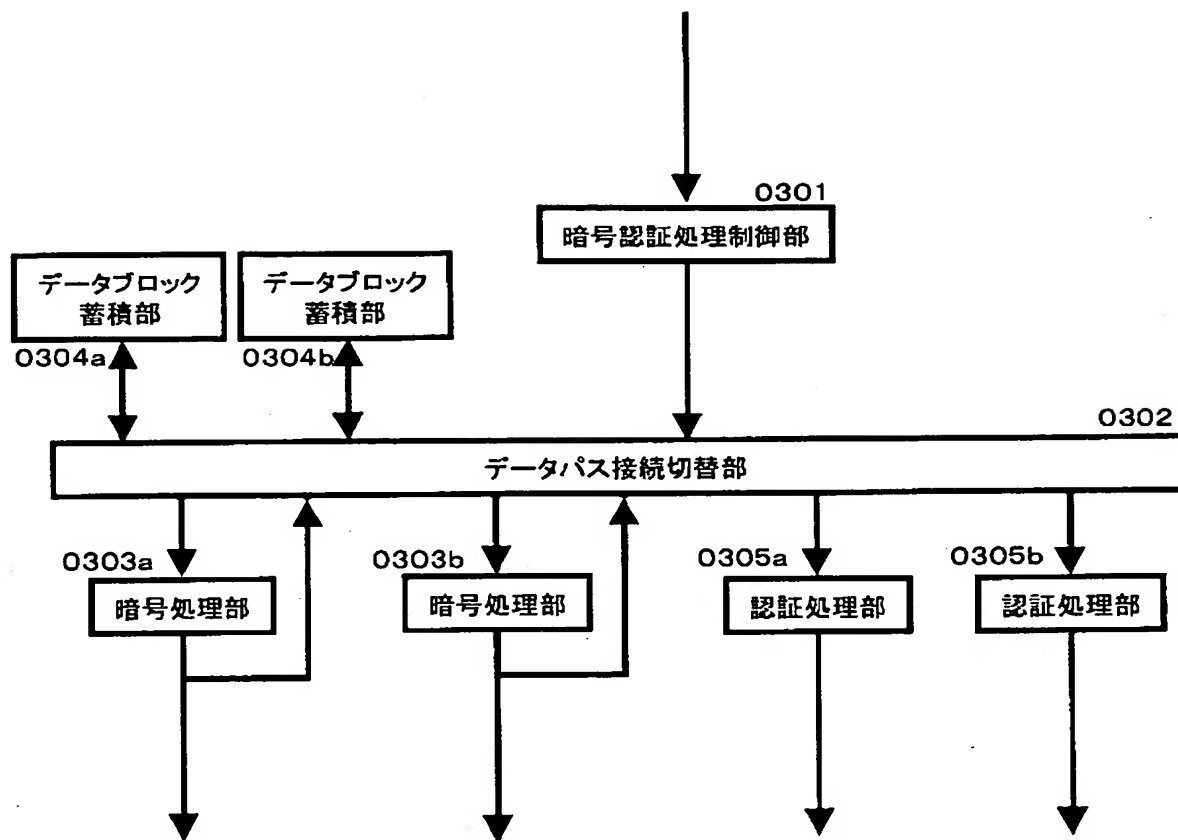
【図 1】



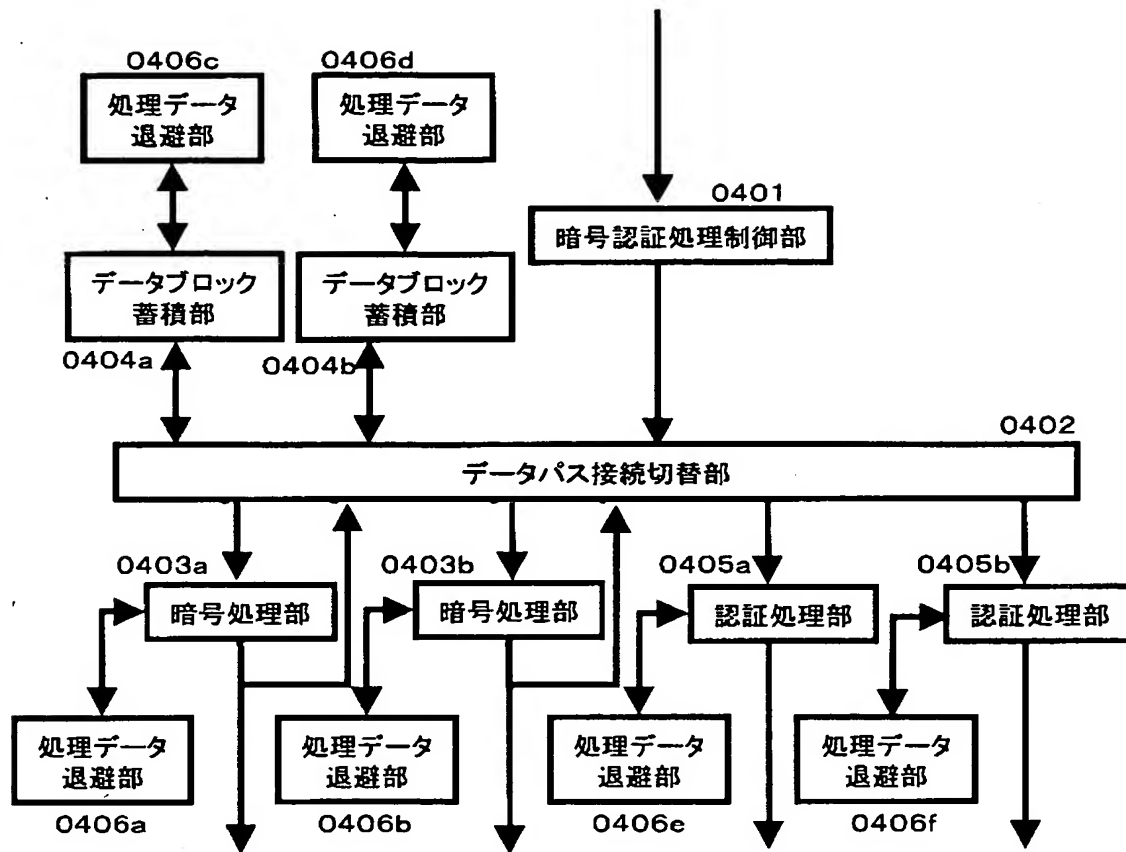
【図 2】



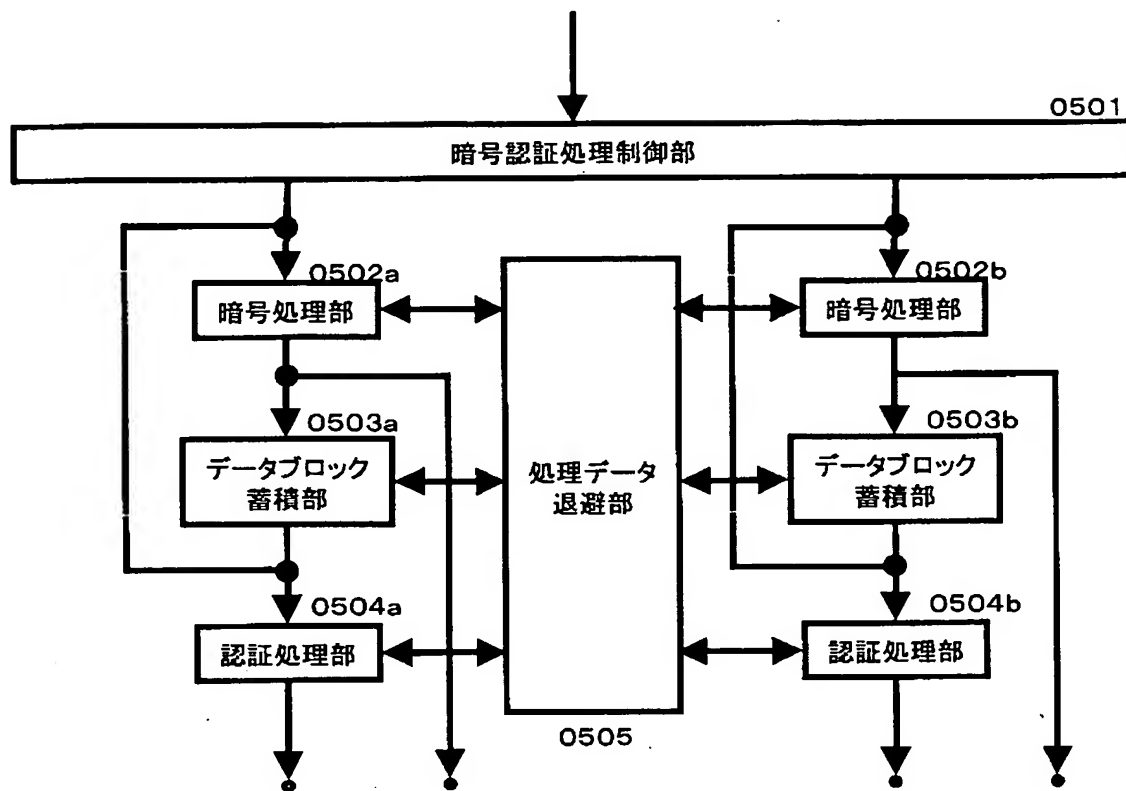
【図 3】



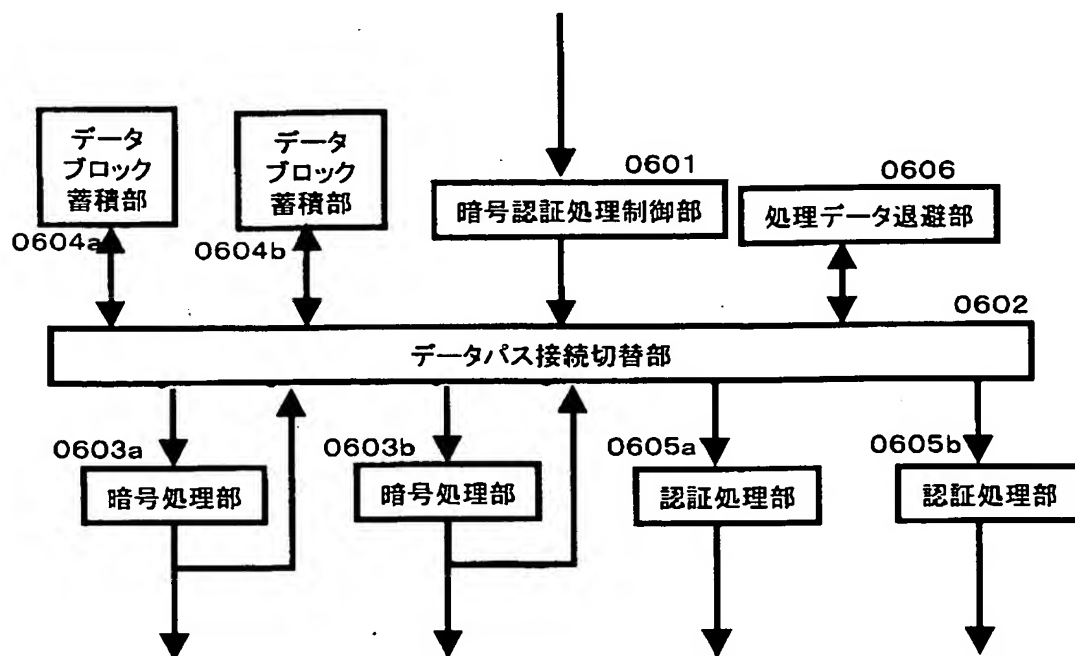
【図 4】



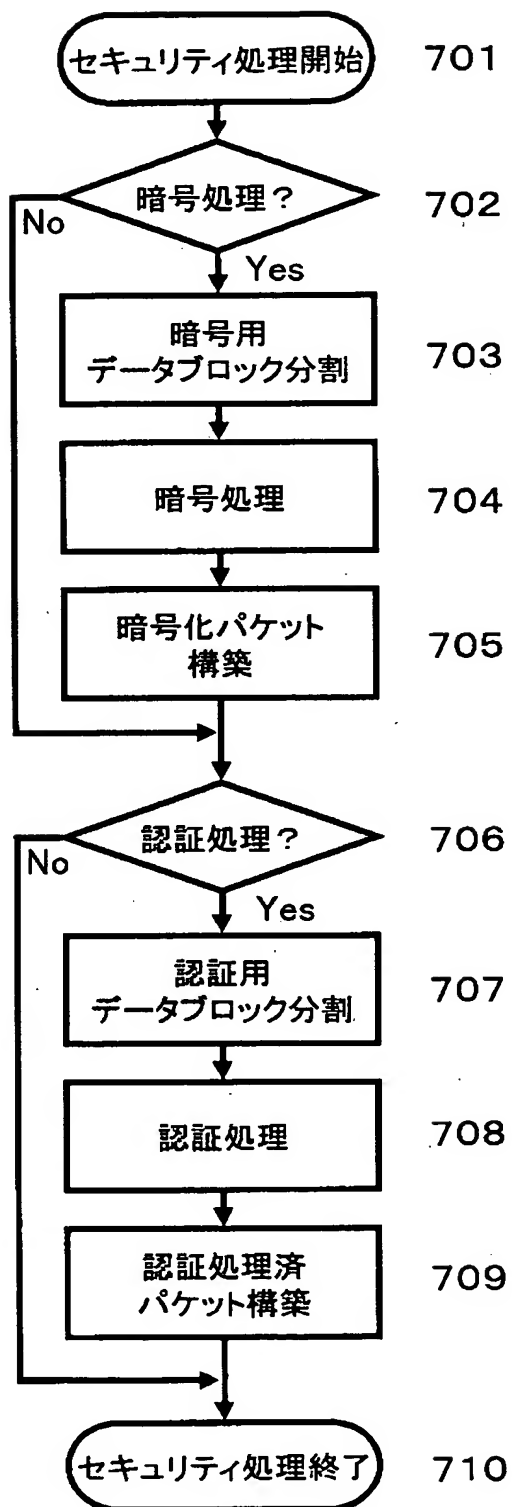
【図 5】



【図 6】



【図 7】





【書類名】 要約書

【要約】

【課題】 秘密通信時のパケットの暗号および認証処理について、その処理単位をパケットから暗号および認証処理に必要十分なデータブロックとすることにより、処理速度およびスループットの向上、低遅延処理、暗号処理部および認証処理部のより効率的な使用を目的とする。

【解決手段】 暗号および認証の両処理を必要とするパケットについて、暗号処理部 0 1 0 2 で処理されたデータブロックを、認証処理用データブロックサイズに等しくなるまでデータブロック蓄積部 0 1 0 3 で逐次的に蓄積し、等しくなるとこれを認証処理部 0 1 0 4 に出力し認証処理することにより、処理単位を暗号または認証処理に必要十分なデータブロックサイズにする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社